WHAT IS CLAIMED IS:

1. A cipher designing apparatus for designing cipher logic of a cipher device that effects cipher or decryption per block by using an F-function for converting input bits to output bits by means of a plurality of S-boxes, said cipher designing apparatus comprising:

a selecting unit which selects an input and output bit number of said plurality of S-boxes based on a memory capacity of a high-speed referable memory provided to said cipher device; and

a S-box generating unit which generates a plurality of S-boxes each having the input and output bit number selected by said selecting unit.

2. The cipher designing apparatus according to claim 1, further comprising a F-function generating unit which generates an F-function having said plurality of S-boxes generated by said S-box generating unit.

3. The cipher designing apparatus according to claim 1, wherein said selecting unit selects the input and output bit number of each S-box in such a manner that a sum of sizes of said plurality of S-boxes becomes largest within a memory capacity of a primary cache memory installed in a processor provided to said cipher device.

4. The cipher designing apparatus according to claim 3, wherein said selecting unit includes:

an input unit which inputs the memory capacity of said primary cache memory and an entire input and output bit number of said block;

a tentative decision unit which tentatively decides an input and output number of each S-box by generating an input and output number of each S-box by dividing the entire input and output bit number of said block inputted from said input unit and allocating a remainder to the input and output number of an arbitrary S-box; and

a combining unit which combines the input and output numbers of the S-boxes tentatively decided by said tentative decision unit within the memory capacity of said primary cache memory.

5. The cipher designing apparatus according to claim 1, further comprising a smallest input and output number specifying unit which specifies a smallest value of the input and output number of said plurality of S-boxes.

6. The cipher designing apparatus according to claim 4, wherein said combining unit completes combining of the input and output numbers based on a final value determined by the entire input and output bit number of said block and the

memory capacity of said primary cache memory.

7. The cipher designing apparatus according to claim 4, wherein said tentative decision unit tentatively decides the input and output number of each S-box by allocating said remainder, if there is any, to the input and output numbers of the S-boxes that are placed apart at remotest positions.

8. A cipher designing method for designing cipher logic of a cipher device that effects cipher or decryption per block by using an F-function for converting input bits to output bits by means of a plurality of S-boxes, the method comprising the steps of:

selecting an input and output bit number of said plurality of S-boxes based on a memory capacity of a high-speed referable memory provided to said cipher device; and

generating a plurality of S-boxes each having the input and output bit number selected at the input and output bit number selecting step.

9. The cipher designing method according to claim 8, further comprising the step of generating an F-function having said plurality of S-boxes generated at the S-boxes generating step.

10. The cipher designing method according to claim 8, wherein, at the input and output bit number selecting step, the input and output bit number of each S-box is selected in such a manner that a sum of sizes of said plurality of S-boxes becomes largest within a memory capacity of a primary cache memory installed in a processor provided to said cipher device.

11. The cipher designing method according to claim 10, wherein the input and output bit number selecting step includes the steps of:

inputting the memory capacity of said primary cache memory and an entire input and output bit number of said block;

tentatively deciding an input and output number of each S-box by generating an input and output number of each S-box by dividing the entire input and output bit number of said block inputted in the memory capacity inputting step and allocating a remainder to the input and output number of an arbitrary S-box; and

combining the input and output numbers of the S-boxes tentatively decided at the tentatively deciding step within the memory capacity of said primary cache memory.

12. The cipher designing method according to claim 8, further comprising the step of specifying a smallest value of the input and output number of said plurality of S-boxes.

13. The cipher designing method according to claim 11, wherein combining at the combining step is completed based on a final value determined by the entire input and output bit number of said block and the memory capacity of said primary cache memory.

14. The cipher designing method according to claim 11, wherein, at the tentatively deciding step, the input and output number of each S-box is tentatively decided by allocating said remainder, if there is any, to the input and output numbers of the S-boxes that are placed apart at remotest positions.

15. A computer readable medium for storing instructions, which when executed by a computer, causes the computer to realizes a cipher designing method for designing cipher logic of a cipher device that effects cipher or decryption per block by using an F-function for converting input bits to output bits by means of a plurality of S-boxes, the method comprising the steps of:

selecting an input and output bit number of said

plurality of S-boxes based on a memory capacity of a high-speed referable memory provided to said cipher device; and

generating a plurality of S-boxes each having the input and output bit number selected at said selecting step.